METHOD FOR SENDING SECURITY PROTECTION MESSAGE IN COMMUNICATION SYSTEM

Publication number: JP10191459 (A)

Publication date: 1998-07-21

Inventor(s): LUO TIE + (LUO TIE)

Applicant(s): NOKIA MOBILE PHONES LTD + (NOKIA MOBILE PHONES LTD)

Classification:

- international: H04L9/30; H04Q7/38; H04L9/28; H04Q7/38; (IPC1-7): H04L9/30; H04Q7/38

- European: H04L9/30F

Application number: JP19970304553 19971106

Priority number(s): US19960744682 19961106

Abstract of JP 10191459 (A)

PROBLEM TO BE SOLVED: To send a security protection message by using a public encryption key. SOLUTION: A transmitter side uses an own public encryption key Ex to encrypt a message (c) and sends the encrypted message Ex (c) to a receiver side. The receiver side uses an encryption key Ey of an object recipient of the message to encrypt the encrypted message Ex (c) and to make a message Ey (Ex(c)) and sends the message Ey(Ex(c)) to the transmitter side. The transmitter side uses its own secret decoding key to decode the message Ey (Ex(c)) and to make Dx(Ey(Ex(c))=Ey(c) and sends the message Ey(c) to the receiver side. When the receiver side is an object recipient of the message, the receiver side uses its

own decoding key Dy to decode the message and to make Dy(Ey(c))=c and when the receiver side is not an objective recipient of the message, the receiver side sends it to the recipient and the recipient uses its own decoding key Dy to decode the message.

(19)日本国特許庁（ＪＰ）　(12) **公開特許公報（Ａ）**　(11)特許出願公開番号

特開平10－191459

(43)公開日　平成10年(1998)７月21日

(51)Int.Cl.[6]	識別記号	ＦＩ		
Ｈ０４Ｑ　7/38		Ｈ０４Ｂ　7/26		１０９Ｒ
Ｈ０４Ｌ　9/30		Ｈ０４Ｌ　9/00		６６３Ａ
				６６３Ｂ

審査請求　未請求　請求項の数11　ＯＬ　（全 10 頁）

(21)出願番号　特願平9－304553

(22)出願日　平成９年(1997)11月６日

(31)優先権主張番号　０８／７４４６８２

(32)優先日　1996年11月６日

(33)優先権主張国　米国（ＵＳ）

(71)出願人　590005612
ノキア　モービル　フォーンズ　リミティド
フィンランド国，エフアイエヌ－02150　エスポー，ケイララーデンティエ　４

(72)発明者　ティエ　ルオ
アメリカ合衆国，テキサス　76006，アーリントン，サンライト　ドライブ　2606

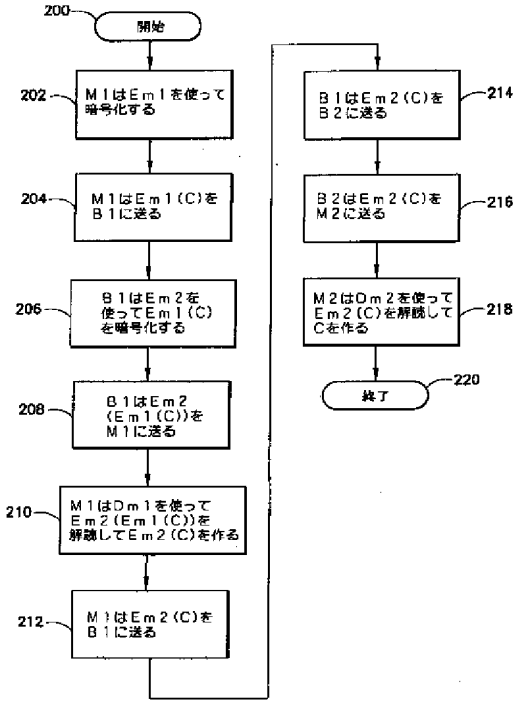
(74)代理人　弁理士　石田　敬　（外３名）

(54)【発明の名称】　通信システムにおいて機密保護メッセージを送る方法

(57)【要約】

【課題】　公開の暗号化キーを用いて機密保護メッセージを送る。

【解決手段】　送信側は自分の公開の暗号化キーExを使ってメッセージｃを暗号化し、その暗号化されたメッセージEx(c)を受信側に送る。受信側は、そのメッセージの目的の受取手の暗号化キーEyを使って暗号化メッセージEx(c)を暗号化してメッセージEy(Ex(c))を作り、このメッセージEy(Ex(c))を送信側に送る。送信側は自分の秘密の解読キーを使ってそのメッセージEy(Ex(c))を解読してDx(Ey(Ex(c)))=Ey(c)を作り、このメッセージEy(c)を受信側に送る。受信側は、自分がそのメッセージの目的の受取手であるならば、自分自身の解読キーＤｙを使ってそのメッセージを解読してDy(Ey(c))=cを作り、自分がそのメッセージの目的の受取手ではなければ、受取手に送り、受取手が自分自身の解読キーDyを使ってそのメッセージを解読する。



【特許請求の範囲】
【請求項１】　少なくとも１つの基地局と複数の移動局とを有する通信システムで機密保護メッセージを送る方法において、前記方法は：各移動局に解読キーと公開の暗号化キーとを割り当て；第１移動局において前記第１移動局の暗号化キーを用いて第１メッセージを暗号化して第２メッセージを作り；前記第２メッセージを前記第１移動局から前記の少なくとも１つの基地局に送り；前記の少なくとも１つの基地局において第２移動局の暗号化キーを用いて前記第２メッセージを暗号化して第３メッセージを作り；前記第３メッセージを前記の少なくとも１つの基地局から前記第１移動局に送り；前記第１移動局において前記第１移動局の解読キーを用いて前記第３メッセージを解読して第４メッセージを作り；前記第４メッセージを前記第１移動局から前記の少なくとも１つの基地局に送り；前記第４メッセージを前記の少なくとも１つの基地局から前記第２移動局に送り；前記第２移動局において前記第２移動局の解読キーを用いて前記第４メッセージを解読して前記第１メッセージを作り直すステップから成ることを特徴とする方法。
【請求項２】　前記第１移動局の解読キー及び暗号化キー、並びに前記第２移動局の解読キー及び暗号化キーは、前記第２移動局の暗号化キーをメッセージに適用して第１結果を得てから前記第１移動局の解読キーをその第１結果に適用して最終結果を得ることが、前記第１移動局の解読キーを前記メッセージに適用して第２結果を得てから前記第２移動局の暗号化キーを前記第２結果に適用して前記最終結果を得ることと同等であるように構成されていることを特徴とする請求項１に記載の方法。
【請求項３】　前記第１移動局において暗号化及び解読を行う前記ステップは第１アルゴリズムに従って行われ、前記第２移動局において暗号化及び解読を行う前記ステップは第２アルゴリズムに従って行われることを特徴とする請求項１に記載の方法。
【請求項４】　前記第１アルゴリズムはＲＳＡ型のアルゴリズムから成り、前記第２アルゴリズムはラビン型のアルゴリズムから成ることを特徴とする請求項３に記載の方法。
【請求項５】　前記第１アルゴリズムはラビン型のアルゴリズムから成り、前記第２アルゴリズムはＲＳＡ型のアルゴリズムから成ることを特徴とする請求項３に記載の方法。
【請求項６】　第１及び第２の送受信装置を有する通信システムで機密保護メッセージを送る方法において、前記方法は：前記の第１及び第２の送受信装置の各々に解読キー及び公開の暗号化キーを割り当て；前記第１送受信装置において前記第１送受信装置の暗号化キーを用いて第１メッセージを暗号化して第２メッセージを作り；前記第２メッセージを前記第１送受信装置から前記第２送受信装置に送り；前記第２送受信装置において前記第２送受信装置の暗号化キーを用いて前記第２メッセージを暗号化して第３メッセージを作り；前記第３メッセージを前記第２送受信装置から前記第１送受信装置に送り；前記第１送受信装置において前記第１送受信装置の解読キーを用いて前記第３メッセージを解読して第４メッセージを作り；前記第４メッセージを前記第１送受信装置から前記第２送受信装置に送り；前記第２送受信装置において前記第４メッセージを解読して前記第１メッセージを作り直すステップから成ることを特徴とする方法。
【請求項７】　前記第１送受信装置の解読キー及び暗号化キー、並びに前記第２送受信装置の解読キー及び暗号化キーは、前記第２送受信装置の暗号化キーをメッセージに適用して第１結果を得てから前記第１送受信装置の解読キーをその第１結果に適用して最終結果を得ることが、前記第１送受信装置の解読キーを前記メッセージに適用して第２結果を得てから前記第２送受信装置の暗号化キーを前記第２結果に適用して前記最終結果を得ることと同等であるように構成されていることを特徴とする請求項６に記載の方法。
【請求項８】　前記第１送受信装置において暗号化及び解読を行う前記ステップは第１アルゴリズムに従って行われ、前記第２送受信装置において暗号化及び解読を行う前記ステップは第２アルゴリズムに従って行われることを特徴とする請求項６に記載の方法。
【請求項９】　前記第１アルゴリズムはＲＳＡ型のアルゴリズムから成り、前記第２アルゴリズムはラビン型のアルゴリズムから成ることを特徴とする請求項８に記載の方法。
【請求項１０】　前記第１アルゴリズムはラビン型のアルゴリズムから成り、前記第２アルゴリズムはＲＳＡ型のアルゴリズムから成ることを特徴とする請求項８に記載の方法。
【請求項１１】　前記第２送受信装置は第１基地局から成り、前記第１送受信装置は第１移動局から成り、前記通信システムは更に第２基地局と第２移動局とを有し、前記方法は更に：前記第１メッセージを前記第１基地局から前記第２基地局に送り；前記第２基地局において前記第２基地局の解読キーを用いて前記第１メッセージを暗号化して第５メッセージを作り；前記第５メッセージを前記第２基地局から前記第２移動局に送り；前記第２移動局において前記第２移動局の暗号化キーを用いて前記第５メッセージを暗号化して第６メッセージを作り；前記第５メッセージを前記第２移動局から前記第２基地局に送り；前記第２基地局において前記第２基地局の解読キーを用いて前記第５メッセージを解読して第７メッセージを作り；前記第７メッセージを前記第２基地局から前記第２移動局に送り；前記第２移動局において前記第２移動局の解読キーを用いて前記第７メッセージを解読して前記第１メッセージを作り直すステップを有する

ことを特徴とする請求項６に記載の方法。
【発明の詳細な説明】
【０００１】
【発明の属する技術分野】本発明は、通信システムのための暗号化技術に関し、特に通信システムにおいて公開の暗号化キーを使用して機密保護メッセージを送る装置及び方法に関する。
【０００２】
【従来の技術】通信システム技術が進歩して、いろいろな通信システム及びサービスを利用できるようになっている。それらのシステムの中には、セルラー電話通信網、個人通信システム、種々のページングシステム、及び種々の有線及び無線のデータ通信網が含まれる。今日アメリカ合衆国で使用されているセルラー電話通信網は、ＡＭＰＳアナログシステム、デジタルＩＳ－１３６時分割多重（ＴＤＭＡ）システム、及びデジタルＩＳ－９５デジタル符号分割多重（ＣＤＭＡ）システムを含む。ヨーロッパでは、移動通信用広域（ＧＳＭ）デジタルシステムが最も広く使用されている。これらのセルラーシステムは８００－９００ＭＨｚの範囲で動作する。個人通信システム（ＰＣＳ）も合衆国で現在展開されている。多くのＰＣＳシステムが１８００－１９００ＭＨｚ範囲に対して開発されつつあるが、それらは各々主要なセルラー規格のうちの１つに基づいている。
【０００３】上記の通信システムの各々において、該システムのオペレータがシステムのユーザーに機密保護通信手段を提供することが望ましいことがしばしばある。それは、該システムで動作している２つの移動局の間で機密保護メッセージを送ることを含むことがある。多くの場合にそのメッセージはテキストメッセージ等の、有限の長さのテキストメッセージである。
【０００４】ＡＭＰＳ等のアナログシステムでは、通信内容を機密保護するのは非常に難しい。２ユーザー間で通信内容を運ぶ信号がアナログの性質であるために暗号化を簡単にも効率的にも行うことはできない。実際、標準的ＡＭＰＳでは、暗号化は全く行われず、移動局と基地局との間で送られる通信メッセージは監視されたり傍受されたりされ得る。通信チャネルに使用される周波数に同調させることのできる受信装置を持っているものは誰でも、見つかることなく何時でも通信を傍受することができる。この傍受の可能性は、ＡＭＰＳ等のアナログシステムに結びついた１つの不都合な要素であった。この様に傍受される可能性があるために、ＡＭＰＳ型のシステムは機密保護メッセージを送ることを必要とする或る種のビジネスユーザーや政府筋のユーザーには好まれていない。
【０００５】通信の秘密を目的として暗号化サービスを含むＧＳＭ、ＩＳ－１３６及びＩＳ－９５等の新しいデジタルシステムが開発されている。これらのデジタルシステムで２ユーザー間で通信メッセージを運ぶ音声信号或いはデータ信号はデジタルの性質を持っているので、ランダム或いは疑似ランダムの性質を持っている通信信号を作るための暗号化装置を通して処理され、認可された受信装置で解読される。この様なシステムで機密保護メッセージを送りたいときには、該システムの暗号化機能を使ってメッセージを暗号化することができる。例えば、これらの規格で指定されているショートメッセージサービス（ＳＭＳ）機能を使って、該システムの暗号化アルゴリズムに従って暗号化されているテキストメッセージを送ることができる。
【０００６】ＧＳＭ、ＩＳ－１３６、及びＩＳ－９５システムでは、暗号化は各ユーザーとシステムとの間のメッセージ送信に対して秘密のキー値”非公開キー”を用いて行われ、そのキーはシステムと通信するユーザーとシステムとだけに知られている。ここで検討しているＰＣＳ通信網についてのシステム規格は、特定のＰＣＳ規格の淵源となるデジタル規格、即ちＧＳＭ、ＩＳ－１３６、或いはＩＳ－９５において指定されている暗号化技術に基づく暗号化サービスを包含することもできる。
【０００７】ＧＳＭではシステムのオペレータがシステムの各ユーザーに加入者識別モジュール（ＳＩＭ）を発行することによって機密保護プロセスを制御する。ＳＩＭは、ユーザーが呼を発したり受けたりするのに使う移動局に挿入しなければならない差し込み式のチップ又はカードである。ＳＩＭは、各ユーザーに独特の、Ｋｉと呼ばれる１２８ビットの数を内蔵している。このＫｉは、確認と、暗号化キーの導出との両方のために使われる。ＧＳＭでは、各ユーザーを確認してそのユーザーについてのＫｉから暗号化ビットを作成するために呼びかけと応答の手続が使われる。この呼びかけと応答の手続をホームシステムの自由裁量で実行することができる。
【０００８】ＧＳＭ移動局が自分のホームシステムで動作しているとき、ユーザーが自分の国際移動システム識別子／一時移動システム識別子（international mobile system identity/temporary mobile system identities（IMSI/TMSI））を呈示することによって自分が誰であるかを明らかにした後、該システムで１２８ビットの乱数（ＲＡＮＤ）が作成されてその移動局のユーザーのＫｉと結合されて３２ビットの応答（ＳＲＥＳ）となる。このときシステムはＲＡＮＤを該移動局に送り、該移動局はそのユーザーのＫｉから自分自身のＳＲＥＳ値を計算し、このＲＡＮＤをシステムに送り戻す。もしその２つのＳＲＥＳが調和するならば、その移動局は本物であると判断される。暗号化キー”Ｋｃ”を作るために、該移動局及び通信網の両方においてＲＡＮＤ及びＫｉを使用するアルゴリズムにより、該移動局とシステムとの間の通信のための暗号化ビットが作成される。その後、Ｋｃは両端で機密保護通信を行うために使用される。ＧＳＭ移動局が移動中であるとき、該移動局が訪れたシステムにおいて該ユーザーの登録が行われるときに、或いは

ユーザーが訪れたシステムから特別の要求が行われたときに、そのシステムにＲＡＮＤ、ＳＲＥＳ及びＫｃの値が転送される。Ｋｉ値はホームシステム及びユーザーのＳＩＭ以外では決して使用し得ない。

【０００９】ＩＳ－１３６及びＩＳ－９５の確認及び暗号化の処理手順は互いに同一であり、またＧＳＭの確認及び暗号化の処理手順と似ている。ＩＳ－１３６システム及びＩＳ－９５システムでは、呼びかけと応答の方法も利用される。そのＩＳ－１３６及びＩＳ－９５の方法は、”Ａキー”と呼ばれる機密保護キーを利用する。各移動局についての６４ビットのＡキーはシステムのオペレータによって決定される。各移動局についてのＡキーはその移動局の所有者のホームシステムとその移動局自体とに記憶される。最初にＡキーは米国郵便等の安全な方法で移動局の所有者に通知され得る。その所有者はキーパッドを介してそのＡキーを移動局に入力することができる。或いは、Ａキーを工場或いは点検修理の場所で移動局にプログラムすることもできる。Ａキーは、移動局及びホームシムの両方で共有される秘密データ（shared secret data（ＳＳＤ））を所定のアルゴリズムから作成するために使われる。各移動局についてのＳＳＤは、ホームシステムのオペレータのみが開始することのできるオーバーエア・プロトコル（an over the airprotocol）の使用によってその移動局のＡキーから定期的に導出され更新され得る。

【００１０】ＩＳ－１３６及びＩＳ－９５の確認及び暗号化では、３２ビットの広域呼び掛けが該移動局のサービスエリアのシステム内で所定間隔をおいて作成されて放送される。移動局がホームシステムにおいてシステム登録／呼設定アクセスを試みるとき、該移動局においてそのＳＳＤから１８ビットの確認応答を計算するために現在の広域呼び掛け応答が使用される。その後、その確認応答とその移動局についての呼カウント値とを含むアクセス要求メッセージが該移動局からホームシステムに送られる。そのアクセス要求を受け取ると、ホームシステムは広域呼び掛け及びその移動局のＳＳＤを使ってそれ自身の応答値を計算する。確認応答と、その移動局のＳＳＤと、呼カウント値を含む他の関連データとの比較によって、その移動局が本物であると確認されれば、その移動局は登録される。

【００１１】移動局が訪問先のシステムでシステム登録／呼設定アクセスを試みるとき、現在の広域呼び掛け応答を用いて該移動局において該移動局のＳＳＤから１８ビットの確認応答を計算する。次にアクセス要求メッセージが該移動局から訪問先のシステムに送られる。訪問先のシステムでの初期登録アクセスについては、アクセス要求メッセージは移動局で計算された確認応答を含む。確認応答と広域呼び掛けとは該移動局のホームシステムに送られ、該ホームシステムはその広域呼び掛けと該移動局のＳＳＤとを使ってそれ自身の応答値を計算する。確認応答同士を比較することによってその移動局が本物であると確認されたならば、その移動局のＳＳＤと、呼カウント値を含む他の関連データとが訪問先のシステムに送られて該移動局が登録される。該移動局が関わる呼が設定されるとき、現在の確認応答値と呼カウントとが該移動局から呼設定情報とともに該システムに送られる。呼設定情報を受け取ると、訪問先のシステムは、要求をしている移動局についての記憶されているＳＳＤと呼カウント値とを検索する。その後、訪問先のシステムは、受け取ったＳＳＤ値と現在の広域呼び掛けとが該移動局で作られたのと同じ応答を作ることを確かめるために確認応答値を計算する。もしその確認応答同士と呼カウント同士とが揃うならば、その移動局は呼アクセスを許可される。通信の機密保護が希望される場合には、暗号化キー・ビットを作成するために広域呼び掛けと該移動局のＳＳＤとを入力として用いて暗号化キーが該移動局とシステムとの両方で作成される。

【００１２】ＧＳＭ、ＩＳ－１３６及びＩＳ－９５システムで使用されるような技術についての更なる背景情報が”ＩＥＥＥ個人通信”の６－１０頁の１９９５年８月付けのダン・ブラウンによる”個人通信システムにおけるプライバシー及び確認のための技術”という論文（the article ”Techniques for Privacy and Authentication in Personal Communications Systems” by Dan Brown in IEEE Personal Communications, dated August 1995, at pages 6-10 ）に開示されている。

【００１３】ＧＳＭ、ＩＳ－１３６及びＩＳ－９５システムで使用される上記の機密キー処理手順は通信の機密を保護するものであるけれども、これらの処理手順のいずれも、傍受及び盗聴を完全に免れ得るわけではない。これらの処理手順の全てが、ユーザーのＡキー又はＫｉ値が移動局とホームシステムとの双方に知られていることを必要とする。これらの処理手順は、ユーザーのＳＳＤ又はＫｃ値が通信リンクの両端即ちシステム及び移動局の双方において知られていることをも必要とする。これらの各値がもしかすると改悪されて傍受者に知られてしまっているという可能性もあり得る。ユーザーのＫｉ又はＡキーを知っている人、或いはシステム間通信をしているユーザーのＫｃ又はＳＳＤを傍受した人は、機密保護されるべき通信を傍受し盗聴する可能性がある。また、各ユーザーのキーは、該ユーザーが通信をする基地局で利用可能であるので、システムの基地局を通して接続している２つの移動局が関わる暗号化通信がその基地局で破られる可能性がある。

【００１４】公開キー暗号化方法は、ユーザーに公開の、即ち公然と知られ明らかにされるかも知れない暗号化キーが割り当てられるけれども、またそのユーザーにしか知られない秘密の解読キーもユーザーに割り当てられるようになっている方法である。目的の受信側ユーザーの解読キーだけがそのユーザーに宛てられた暗号化さ

れたメッセージを解読することができる、即ちその目的の受信側ユーザーの暗号化キーを使って暗号化されたメッセージを解読することができる。公開キー暗号化通信システムでは、ユーザーは解読キーを基地局やシステムから隠して自分で保管しておくことを許されるであろう。メッセージを解読するのに必要なキーを知っているのは受信側のユーザーだけであるので、公開キー暗号化方法は、例えばＧＳＭ、ＩＳ－１３６、或いはＩＳ－９５で使われている現在の暗号化技術で得られるよりも一層安全な通信を提供することができる。

【００１５】在来の公開キー暗号化方法を使用するセルラーシステムでは、移動局Ｘが暗号化されたメッセージを移動局Ｙに送るとすると、移動局Ｘは、移動局Ｙのための公開暗号化キーと、移動局Ｙの暗号化キーとともに使用されなければならないアルゴリズムとの両方を知る必要がある。移動局Ｘが移動局Ｙの暗号化キーとアルゴリズムとを使ってメッセージを暗号化することができることも必要であろう。在来の公開キー暗号化方法のこれらの要件は、場合によってはセルラーシステムで使用するに当たって或る種の困難を引き起こしたり、或いは余り適していないかも知れない。

【００１６】

【発明が解決しようとする課題】公開キー暗号化法を使用するに当たっての１つの難点は、暗号化と解読とに必要な計算が秘密キーシステムで必要とされるよりも遥かに多量の計算資源を必要とするかも知れないことである。移動局ではその様な計算資源には限りがあるかも知れない。二人の移動局ユーザーが各々異なる暗号化／解読アルゴリズムを使ってメッセージを秘密裏に交換したいと望む場合には資源に関する要件はもっと大きくなり得る。例えば、移動中の移動局のホームシステムのアルゴリズムとは異なる自分独自のアルゴリズムを実行するための手段をシステムオペレータが備えているシステムにその移動中の移動局が入り込んだときなどには、前記のように資源に関する要件が大きくなるかも知れない。この場合、どの移動局も、他のユーザーのアルゴリズムで暗号化を行うとともにその移動局のユーザーのアルゴリズムで解読を行うことができなければならないであろう。例えば、暗号化するために使われるアルゴリズムが、その暗号化を実行する移動局で利用し得るよりも多量の計算資源を必要とするならば、その様な要件を満たすのは困難であるかも知れない。また、特定のアルゴリズムを実行するためのコード及びデータを各移動局に記憶させておくか或いは暗号化開始前に該移動局に送信しなければならないであろうから、移動局の計算資源に対する要求が更に大きくなる。

【００１７】セルラーシステムで公開キー暗号化法を使用することについてのもう一つの潜在的難点は、メッセージを送信側移動局或いは受信側移動局だけが利用し得ることを保証するために送信側の移動局が受信側移動局の暗号化キーを知っていなければならないということである。或る種の公開キー暗号化法では暗号化キーは各々非常に大きい可能性があり、それは場合によっては数列であり、受信側となる可能性のある全ての移動局のための暗号化キーを１つの移動局に記憶させるのは困難であるかも知れない。受信側の移動局のキーがもし非常に大きければ、例えば呼設定時などに、必要に応じて送信側移動局に送ることも困難であるかも知れない。

【００１８】

【課題を解決するための手段】本発明は、公開キー暗号化法を使用する通信システムにおいて機密保護メッセージを送る方法を提供する。この方法は、ユーザーの解読キーがそのユーザーの送受信装置においてのみ知られることとなるように実施される。この方法は、ユーザーの送受信装置がそのユーザーの暗号化／解読アルゴリズムと暗号化キーとを使用できるだけでよいようにも実施される。これは、特別のシーケンスを用いて２つの送受信装置間でメッセージを交換することにより実行される。この方法は、機密キー法の使用に伴う機密保護問題を回避し、各移動局がそれ自身の公開キー暗号化／解読アルゴリズムのみを実行できるようにする。この方法では、在来の公開キー暗号化法の場合のように送受信装置が目的の受信側送受信装置の暗号化キーとアルゴリズムとを使って暗号化を実行できることを必要としない。従って、送受信装置の計算資源を特定の１つのアルゴリズム向けに最適化することができる。

【００１９】この方法は、各移動局或いは通信網が各々異なる暗号化／解読アルゴリズムを使用する２つの移動局間又は移動局及びセルラー通信網の間で機密保護メッセージが交換されるときに非常に安全なショートメッセージサービス（ＳＭＳ）テレサービスを提供するのに役立つ。この方法は、計算量の比較的に少ない機密キーアルゴリズムを使って音声伝送などの比較的に長い通信を行えるように、通信を行う２つの移動局間で或いは移動局と通信網との間で機密キーを交換するのにも役立つ。また、１つの移動局から他の移動局又は通信網へ機密保護確認符号定数（a secure authenticatication signature ）を送るためにこの方法を使用することもできる。

【００２０】本発明の或る実施例では、２つのユーザー間で交換されるメッセージのポイント間暗号化法が少なくとも１つの基地局と複数の移動局とを有する通信システムで実施される。このポイント間実施例では、該システムの基地局では解読は行われない。移動局Ｍ１のユーザーには、公然と知られる（システムに知られる）暗号化キーＥｍ１と移動局Ｍ１においてのみ知られる解読キーＤｍ１とが割り当てられる（”暗号化キーＥｍｘ”及び”解読キーＤｍｘ”という用語は、ここではアルゴリズムとそのアルゴリズムで使用されるキー値との両方を指す、即ちＥｍｘは暗号化キー値を使用する暗号化／解読アルゴリズムであり、Ｄｍｘは解読キー値を使用する

暗号化／解読アルゴリズムである）。移動局Ｍ２の他のシステムユーザーには、公然と知られる暗号化キーＥｍ２と、移動局Ｍ２においてのみ知られる解読キーＤｍ２とが割り当てられ、ここでＤｍ１Ｅｍ２＝Ｅｍ２Ｄｍ１である。Ｄｍ１Ｅｍ２＝Ｅｍ２Ｄｍ１は、始めにＤｍ１をメッセージに適用し次にＥｍ２を適用するということは始めにＥｍ２を次にＤｍ１をメッセージに適用することと同じであるという制限を課すものである。Ｍ１のみがＤｍ１を知っており、Ｍ２のみがＤｍ２を知っている。また、Ｍ１はＥｍ１とＭ１の特別の暗号化／解読アルゴリズム（Ａ１）とを知っているだけで良く、Ｍ２はＥｍ２とＭ２の特別の暗号化アルゴリズム（Ａ２）とを知っているだけで良い。

【００２１】移動局Ｍ１を持っているユーザーが移動局Ｍ２のユーザーに機密保護通信メッセージｃを送りたいとき、その通信メッセージｃはＭ１においてＥｍ１及びＡ１を用いて暗号化されてメッセージＥｍ１（ｃ）となる。Ｍ１はこのＥｍ１（ｃ）をシステムの基地局Ｂ１に送る。基地局Ｂ１はＥｍ２とＡ２とを用いてＥｍ１（ｃ）を暗号化してメッセージＥｍ２（Ｅｍ１（ｃ））を作成し、それをＭ１に送り戻す。次にＥｍ２（Ｅｍ１（ｃ））はＭ１においてＤｍ１及びＡ１を用いて解読される。Ｄｍ１Ｅｍ２＝Ｅｍ２Ｄｍ１であるので、Ｄｍ１を用いてＥｍ２（Ｅｍ１（ｃ））を解読するとＥｍ２（ｃ）が得られる。Ｍ１はＥｍ２（ｃ）をＢ１に送る。Ｂ１は、移動局Ｍ２が存在している区域を管理する基地局Ｂ２にＥｍ２（ｃ）を送る。次にＥｍ２（ｃ）は移動局Ｍ２に送られて移動局Ｍ２によってＤｍ２及びＡ２で解読されて、移動局Ｍ１から移動局Ｍ２に送られた通信メッセージｃと成る。

【００２２】本発明の他の実施例では、２つの移動局間での非ポイント間暗号化法が通信システムで実施される。移動局Ｍ１のシステムユーザーには、公然と知られる（システムに知られる）暗号化キーＥｍ１と、移動局Ｍ１においてのみ知られる解読キーＤｍ１とが割り当てられる。Ｍ１は暗号化／解読アルゴリズムＡ１を使用する。移動局Ｍ２の他のシステムユーザーには、公然と知られる暗号化キーＥｍ２と、移動局Ｍ２においてのみ知られる解読キーＤｍ２とが割り当てられる。Ｍ２は暗号化／解読アルゴリズムＡ２を使用する。また、システムの各基地局Ｂｘには、公然と知られる暗号化キーＥｂｘと基地局Ｂｘのみが知る解読キーＤｂｘとが割り当てられる。各基地局はアルゴリズムＡｂｘに従って暗号化／解読を行う。キーは、互いに通信する基地局Ｂｘと移動局Ｍｘとのいずれの対についてもＤｍｘＥｂｘ＝ＥｂｘＤｍｘとなるように選択される。

【００２３】この実施例では、移動局Ｍ１を持っているユーザーが機密保護通信メッセージｃを移動局Ｍ２のユーザーに送ることを望んでいるとき、通信メッセージｃはＭ１でＥｍ１及びＡ１を用いて暗号化されてメッセージＥｍ１（ｃ）となる。Ｍ１はこのＥｍ１（ｃ）をシステムの基地局Ｂ１に送る。基地局Ｂ１はＥｂ１及びＡｂ１を用いてＥｍ１（ｃ）を暗号化してメッセージＥｂ１（Ｅｍ１（ｃ））を作り、それをＭ１に送る。Ｅｂ１（Ｅｍ１（ｃ））は次にＭ１においてＤｍ１及びＡｍ１を用いて解読される。Ｄｍ１Ｅｂ２＝Ｅｂ２Ｄｍ１であるので、Ｄｍ１を用いてＥｂ１（Ｅｍ１（ｃ））を解読するとＥｂ１（ｃ）が得られる。次にＭ１はＥｂ１（ｃ）をＢ１に送る。Ｂ１は、Ｄｂ１及びＡｂ１を用いてＥｂ１（ｃ）を解読してｃを作り、移動局Ｍ２が位置している地域を管理する基地局Ｂ２にｃを送る。次にＢ２とＭ２との間で通信メッセージｃはＭ１とＢ１との間での転送について述べたのと全く同様に暗号化されるが、この場合、Ｂ２、Ｅｂ２、Ｄｂ２及びＡｂ２がＭ１、Ｅｍ１、Ｄｍ１及びＡｍ１に代わり、Ｍ２、Ｅｍ２、Ｄｍ２及びＡｍ２がＢ１、Ｅｂ１、Ｄｂ１及びＡｂ１に代わる。

【００２４】以下の詳細な説明を添付図面と関連させて読めば本発明の方法を一層充分に理解できる。

【００２５】

【発明の実施の形態】図１は本発明の実施例に従って構成された通信システム１００のブロック図である。システム１００は、基地局Ｂ１及びＢ２、陸線通信網１４２、及び移動局Ｍ１及びＭ２から成る。２つの基地局と２つの移動局とを包含するものとして図示されているけれども、システム１００は図１に示されているより多数或いは少数の基地局或いは移動局から成っていてもよい。移動局Ｍ１及びＭ２は、Ｍ１又はＭ２のユーザーと他の移動電話との間、或いはユーザーと陸線通信網１４２に接続された陸線電話との間で音声通信を提供する移動電話であってもよい。移動局Ｍ１及びＭ２は、個人通信装置或いは無線モデムを通して動作するラップトップ型コンピュータなどの、システム１００についてのシステム規格に従って動作することのできる他の随意の種類の移動通信装置であってもよい。陸線通信網１４２は、公衆交換電話回線網（ＰＳＴＮ）、或いは、呼経路選択、登録、及びシステム１００内での移動局の１つの基地局から他の基地局へのハンドオフを制御するための移動交換センターを包含するシステム１００のための私設陸線通信網であってもよい。システム１００では、移動局Ｍ１及びＭ２はＲＦリンクを通してシステム１００の基地局と通信しながらシステム１００の通達範囲の中を動き回ることができる。図１では、移動局Ｍ１及びＭ２は、それぞれＲＦリンク１４４及び１４６を介して基地局Ｂ１及びＢ２とそれぞれ通信しているものとして示されている。システム１００は、ＲＦリンクを介して移動局Ｍ１及びＭ２と基地局Ｂ１及びＢ２との間にデジタルインターフェースを提供する如何なる通信システム規格に従って動作してもよい。デジタル通信システムの設計及び動作は公知であるので、ここでは詳しくは説明しな

い。システム１００はいろいろな方法で具体化され得る。例えば、システム１００のデジタルＲＦインターフェースは、通信産業協会／電子産業協会（(Telecommunications Industry Association/Electronic Industry Association（ＴＩＥ／ＥＩＡ））のＩＳ－１３６、ＩＳ－９５、及びＰＣＳ１９００規格或いはＧＳＭ規格に類似する規格に従って動作することができる。

【００２６】移動局Ｍ１は、システム１００の基地局と無線信号をやりとりするためのアンテナ１０２に結合されたトランシーバー・ユニット１０４を包含している。移動局Ｍ１はユーザーインターフェース１０８を包含しているが、それはコンピュータ・キーボードであるか、或いはキーパッド、マイクロホン及び受話口の付いている移動電話の送受器であり得る。移動局Ｍ１の制御ユニット１０６は、ＲＦチャネル選択及びその他のシステム機能を通常の方法で制御し、論理ユニット１１２は該移動局の全般的動作を制御する。通信の機密保護を行うために使われる暗号化及び解読の機能を実現し実行するためにも論理ユニット１１２を利用することができる。ディスプレイ１１０は、移動局Ｍ１のユーザーに総合的視覚インターフェースを提供するものであり、論理ユニット１１２により制御される。移動局Ｍ２はトランシーバー・ユニット１１６、ユーザーインターフェース１２０、制御ユニット１１８、論理ユニット１２４、及びディスプレイ１２２を包含しており、これらは各々移動局Ｍ１の対応するセクションについて記載したのと同じ機能を持っている。

【００２７】基地局Ｂ１は移動局と無線信号をやりとりするためのアンテナ１３４に結合されたトランシーバー・ユニット１３６を包含している。Ｂ１は制御ユニット１３８及び処理装置１４０も包含している。制御ユニット１３８は、移動局への適当な制御メッセージを作成することによってＲＦチャネル選択及び割り当てを制御するとともに、陸線通信網１４２とのインターフェーシングなどの他の所要のシステム機能も制御する。通信の機密保護のために使われる暗号化及び解読の機能を実現し実行するために処理装置１４０を利用することができる。基地局Ｂ２はトランシーバー・ユニット１２８、アンテナ１２６、制御ユニット１３０及び処理装置１３２を包含しており、これらは各々基地局Ｂ１の対応するセクションについて説明した機能を持っている。

【００２８】本発明の１つの実施例では、暗号化されたメッセージをシステム１００において途中で解読されることなく１つのユーザーから他のユーザーに渡すことができる。２移動局間、基地局及び移動局の間、及び、移動局と適宜の装備を持った陸線加入者局との間を含む、システム内の随意の２ポイント間でのポイント間通信を提供するためにこの実施例を使用することができる。

【００２９】ポイント間メッセージ伝送を安全に行うために、システム１００の各移動局Ｍｘに、公然と知られる暗号化キーＥｍｘと移動局Ｍｘにおいてのみ知られる解読キーＤｍｘとが割り当てられる。通信を希望している任意の２移動局Ｍ１及びＭ２について、Ｄｍ１Ｅｍ２はＥｍ２Ｄｍ１と等しくなければならない。しかし、Ｍ１及びＭ２の各々により使用される暗号化アルゴリズムは異なっていてもよい。ＭＳ１のユーザーがＭＳ２のユーザーに機密保護通信メッセージｃを送ることを希望しているとき、通信メッセージｃはＭＳ１においてＥｍ１及びＡｍ１で暗号化されて暗号化メッセージＥｍ１（ｃ）が作られる。ＭＳ１はこのＥｍ１（ｃ）をシステムの基地局Ｂ１に送る。基地局Ｂ１はＥｍ２及びＡｍ２を用いてＥｍ１（ｃ）を暗号化してメッセージＥｍ２（Ｅｍ１（ｃ））を作り、これをＭＳ１に送る。次にＭＳ１はＤｍ１及びＡｍ１を用いてＥｍ２（Ｅｍ１（ｃ））を解読する。Ｄｍ１Ｅｍ２＝Ｅｍ２Ｄｍ１であるので、Ｄｍ１を用いてＥｍ２（Ｅｍ１（ｃ））を解読するとＥｍ２（ｃ）が得られる。ＭＳ１はこのＥｍ２（ｃ）をＢ１に送る。Ｂ１はこのＥｍ２（ｃ）を、ＭＳ２が位置している地域を管理する基地局Ｂ２に送る。次にＥｍ２（ｃ）はＭＳ２に送られて、ＭＳ２によってＤｍ２及びＡｍ２で解読されて、ＭＳ１によりＭＳ２に送られる解読済み通信メッセージｃが作られる。

【００３０】ここで図２を参照すると、本発明の実施例の通信システム内でポイント間暗号化通信を行うために実行されるプロセスステップを示す流れ図が示されている。実例として、図１の移動局Ｍ１と移動局Ｍ２との間の暗号化メッセージ転送の場合を用いてこのプロセスを説明するが、Ｍ１はラビンのアルゴリズム（Rabin algorithm ）を使用し、Ｍ２はライベスト、シャミル及びエイドルマン（ＲＳＡ）のアルゴリズム（Rivest, Shamir and Adleman (RSA) algorithm）を使用する。ラビンのアルゴリズムについての予備的説明が、１９９５年にＣＲＣにより刊行されたスティンソン（Stinson ）の書籍”暗号法の理論と実際”（”Cryptography, Theory and Practice”）の１４３－１４８頁に記載されている。ＲＳＡアルゴリズムについての詳しい解説が１９９６年にジョン・ワイリイ・アンド・サンズ（John Wiley and Sons ）から刊行されたリンチ等（Lynch et al.）の書籍”デジタルマネー”（”Digital Money”）の７６－８６頁に記載されている。

【００３１】移動局Ｍ１のためのキー関数Ｅｍ１及びＤｍ１をラビンの基準に従って選択することができる。ラビンのアルゴリズムでは、この例では、選択された所定の数Ｎを用いて２つの素数ｐ及びｑが選択され、ここでｐ×ｑ＝Ｎであり、ｐ＝４ｋ１＋３であり、ｑ＝４ｋ２＋３であり、このｋ１及びｋ２は定数である。Ｎは公然と知られてもよいが、ｐ及びｑは秘密に保たれなければならない。Ｅｍ１はＥｍ１（ｃ）＝（ｃ）^{2} ｍｏｄ　Ｎと定義され、ＤＭ１はＤＭ１（ｃ）＝ｃ$^{1/2}$ ｍｏｄ　Ｎと定義され、このｃは送信されるべきメッセージであ

る。ＤＭ１（ｃ）を$c^{1/2}$について解くために、解ｘ１＝±$c^{(p+1)/4}$、及びｘ２＝±$c^{(q+1)/4}$を用いて方程式x^2＝ｃ　ｍｏｄ　ｐとx^2＝ｃ　ｍｏｄ　ｑとを解く。２つの値ａ及びｂがａｐ＋ｂｑ＝１となることが分かったならば、方程式$c^{1/2}$＝ｂｑｘ１＋ａｐｘ２　ｍｏｄ　Ｎによって$c^{1/2}$を発見することができる。

【００３２】移動局Ｍ２についてのキー関数Ｅｍ２、Ｄｍ２をライベスト、シャミル及びエイドルマン（ＲＳＡ）の基準に従って選択することができる。ＲＳＡでは２つの（大きな）素数ｐ及びｑが始めに選択され、ここでｐ×ｑ＝Ｎである。この実施例では、Ｍ２のためのの　ＮはＭ１のために使われるＮに等しい。それ故にＤｍ１Ｅｍ２＝Ｄｍ２Ｅｍ１という条件を満たすのが簡単である。しかし、Ｄｍ１Ｅｍ２＝Ｅｍ２Ｄｍ１である限りは、Ｎの他の値を使ってもよい。その場合、２つの他の値ａ２及びｂ２が選択され、ここで（ａ２）（ｂ２）＝１　ｍｏｄ　（ｐ－１）（ｑ－１）である。Ｎ及びａ２は公開されてもよく、ｂ２は秘密に保たれなければならない。このとき、Ｅｍ２及びＤｍ２はＥｍ２（ｃ）＝（ｃ）^{a2}　ｍｏｄＮ、及びＤｍ２＝（ｃ）^{b2}ｍｏｄ　Ｎと定義される。

【００３３】プロセスはステップ２００から始まり、ここで暗号化プロセスがＭ１で開始される。ステップ２０２において、Ｅｍ１及びＡｍ１を用いて論理ユニット１１２により通信メッセージｃが暗号化されて暗号化メッセージＥｍ１（ｃ）＝（ｃ）^{2}　ｍｏｄ　Ｎが作られる。プロセスはステップ２０４に移行し、ここでＥｍ１（ｃ）はトランシーバー・ユニット１０４を通してＭ１からＢ１へ送信される。トランシーバー・ユニット１３６を通してＥｍ１（ｃ）を受け取った後、Ｂ１の処理装置１４０はステップ２０６でＥｍ２及びＡｍ２を用いてＥｍ１（ｃ）を暗号化して暗号化メッセージＥｍ２（Ｅｍ１（ｃ））＝（（ｃ）^{2}）^{a2}　ｍｏｄＮを作る。プロセスは次にステップ２０８に移り、ここでＥｍ２（Ｅｍ１（ｃ））がＢ１からＭ１に送られる。次にステップ２１０において、Ｂ１からＥｍ２（Ｅｍ１（ｃ））を受け取った後、Ｍ１の論理ユニット１１２は前記の様にＡｍ２（ラビンのアルゴリズム）を用いてＥｍ２（Ｅｍ１（ｃ））を解読する。（Ｅｍ２（Ｅｍ１（ｃ））$^{1/2}$＝（（（ｃ）^{2}）^{a2}）$^{1/2}$である。作られたＤｍ１（Ｅｍ２（Ｅｍ１（ｃ））は（ｃ）^{a2}　ｍｏｄ　Ｎ、即ち暗号化メッセージＥｍ２（ｃ）に等しい。

【００３４】次に、ステップ２１２において、Ｍ１のトランシーバー・ユニット１０４は暗号化メッセージＥｍ２（ｃ）をＢ１に送る。次に、ステップ２１４において、Ｂ１の制御ユニット１３８は陸線通信網１４２を通してＥｍ２（ｃ）をＢ２の制御ユニット１３０に送る。このメッセージは暗号化されているので、これは安全な通信である。次にステップ２１６において、Ｂ２の制御ユニット１３０を通してＥｍ２（ｃ）を受け取った後、トランシーバー・ユニット１２８はＥｍ２（ｃ）をＭ２に送る。ステップ２１８でＥｍ２（ｃ）はＭ２の処理装置１３２でＤｍ２及びＡｍ２を用いて解読されてＤｍ２（Ｅｍ２（ｃ）＝（（ｃ）^{a2}）^{b2}　ｍｏｄＮ、即ちＤｍ２（Ｅｍ２（ｃ））＝ｃが作られる。このときＭ２は解読済み通信メッセージｃを受け取ったことになる。

【００３５】本発明の他の実施例では、システム１００において１つのユーザーから他のユーザーにメッセージを転送するために非ポイント間法が使用される。この実施例では、送信側ユーザーと通信している基地局でそのメッセージが解読される。その後、そのメッセージは該メッセージの受取手と通信している基地局に送られて解読されて該メッセージの受取手に送られる。この実施例では、通信を行っている移動局或いは基地局の各々がそれ自身の暗号化キーと暗号化／解読アルゴリズムとを知っているだけで良い。通信を行っているエンティティーは、通信を行っている他のいずれのエンティティーの暗号化アルゴリズムを知らなくてもよいし、またそれを実行できなくてもよい。

【００３６】一般に、この実施例では、各移動局Ｍｘに暗号化キーＥｍｘと解読キーＤｍｘとが割り当てられる。Ｄｍｘは移動局ｘにおいてのみ知られる。システム１００の各基地局Ｂｘには暗号化キーＥｂｘと解読キーＤｂｘとが割り当てられる。Ｄｂｘは基地局Ｂｘにおいてのみ知られる。互いに通信することを望んでいる移動局Ｍｘ及び基地局Ｂｙの任意の対について、ＤｍｘＥｂｙはＥｂｙＤｍｘに等しくなければならない。

【００３７】Ｍ１のユーザーが機密保護通信メッセージｃをＭ２のユーザーに送ることを望んでいるとき、通信メッセージｃはＭ１によりＥｍ１及びＡｍ１を用いて暗号化されてメッセージＥｍ１（ｃ）が作られる。Ｍ１はこのＥｍ１（ｃ）をシステムの基地局Ｂに送る。その後、基地局Ｂ１はＥｂ１及びＡｂ１を用いてＥｍ１（ｃ）を暗号化してメッセージＥｂ１（Ｅｍ１（ｃ））を作り、これをＭ１に送る。次にＭ１はＤｍ１及びＡ１を用いてＥｂ１（Ｅｍ１（ｃ））を解読する。Ｄｍ１Ｅｂ１＝Ｄｂ１Ｅｍ１であるので、Ｄｍ１及びＡ２を用いてＥｂ１（Ｅｍ１（ｃ））を解読するとＥｂ１（ｃ）が得られる。Ｍ１はこのＥｂ１（ｃ）をＢ１に送る。Ｍ１はこの時点でＢ１に正しいＥｂ１（ｃ）を送る唯一のユーザーであり得る。Ｂ１はＤｂ１及びＡｂ１を用いてＥｂ１（ｃ）を解読してｃを作る。次にＢ１は、システムを通して、ユーザーＭ２が位置している地域を管理する基地局Ｂ２にｃを送る。次にＢ２とＭ２との間で通信メッセージｃはＭ１とＢ１との間での転送について述べたのと全く同様に暗号化され得るが、この場合、Ｂ２、Ｅｂ２、Ｄｂ２及びＡｂ２がＭ１、Ｅｍ１、Ｄｍ１及びＡｍ１に代わり、Ｍ２、Ｅｍ２、Ｄｍ２及びＡｍ２がＢ１、Ｅｂ１、Ｄｂ１及びＡｂ１に代わる。

【００３８】図３を参照すると、本発明の実施例の通信

システム内で非ポイント間暗号化通信を提供するために行われるプロセスステップを示す流れ図が示されている。図３の流れ図を使って、図１の移動局Ｍ１と移動局Ｍ２との間での暗号化メッセージ転送の場合を説明することができる。この例では、Ｍ１及びＭ２はラビンのアルゴリズムを使用し、Ｂ１及びＢ２はＲＳＡアルゴリズムを使用する。図３で使用されるプロセスでは、Ｍ１及びＭ２は基地局で使用されるＲＳＡアルゴリズムを使用しなくてもよい。

【００３９】移動局Ｍｙのキー関数Ｅｍｙ、Ｄｍｙはラビンの基準に従って選択され得る。この例についてのラビンのアルゴリズムでは、選択された数Ｎを用いて２つの素数ｐ及びｑが選択され、ここでｐ×ｑ＝Ｎであり、ｐ＝４ｋ１＋３であり、ｑ＝４ｋ２＋３であり、ｋ１及びｋ２は定数である。Ｎは公然と知られてもよく、ｐ及びｑは秘密に保たれなければならない。ＥｍｙはＥｍｘ（ｃ）＝（ｃ）^{2} ｍｏｄ　Ｎと定義され、ＤＭｙはＤＭｙ（ｃ）＝ｃ$^{1/2}$ｍｏｄ　Ｎと定義される。ＤＭｙ（ｃ）をｃについて解くために、解ｘ１＝±ｃ$^{(p+1)/4}$ 、及び、ｘ２＝±ｃ$^{(q+1)/4}$ を用いて方程式ｘ^{2} ＝ｃ　ｍｏｄ　ｐ、及び、ｘ^{2} ＝ｃ　ｍｏｄ　ｑを解く。２つの値ａ及びｂがａｐ＋ｂｑ＝１であることが分かったならば、方程式ｃ$^{1/2}$ ＝ｂｑｘ１＋ａｐｘ２　ｍｏｄ　Ｎによりｃを見いだすことができる。

【００４０】基地局ｘについてのキー関数Ｅｂｘ及びＤｂｘをライベスト、シャミル及びエイドルマン（ＲＳＡ）の基準に従って選択することができる。ＲＳＡでは、始めに２つの（大きな）素数ｐ及びｑが選択され、ここでｐ×ｑ＝Ｎである。次に他の２つの値ａｘ及びｂｘが選択され、ここで（ａｘ）（ｂｘ）＝１　ｍｏｄ（ｐ－１）（ｑ－１）である。Ｅｂｘ及びＤｂｘは、Ｅｂｘ（ｃ）＝（ｃ）^{ax}　ｍｏｄ　Ｎ、Ｄｂｘ＝（ｃ）^{bx}　ｍｏｄ　Ｎと定義される。この実施例では、Ｂ１についてのＮはＭ１に使用されるＮに等しく、Ｂ２についてのＮはＭ２に使用されるＮに等しい。それ故に、Ｄｍ１Ｅｂ１＝Ｅｂ１Ｄｍ１という条件を満たすのが容易になる。しかし、Ｄｍ１Ｅｂ１＝Ｅｂ１Ｄｍ１であり、且つＤｍ２Ｅｂ２＝Ｅｂ２Ｄｍ２である限りは、Ｎの他の値を使用してもよい。

【００４１】プロセスはステップ３００から始まり、ここで暗号化プロセスが開始される。次にステップ３０２で、通信メッセージｃはＭ１の論理ユニット１１２でＥｍ１及びＡｍ１を用いて暗号化され、暗号化メッセージＥｍ１（ｃ）＝（ｃ）^{2} ｍｏｄ　Ｎが作られる。次にステップ３０４に移行し、ここでＥｍ１（ｃ）はトランシーバー・ユニット１０４を通してＭ１からＢ１に送られる。ステップ３０６で、トランシーバー・ユニット１３６を通してＥｍ１（ｃ）を受け取った後、Ｂ１はＥｂ１及びＡｂ１を用いてＥｍ１（ｃ）を暗号化して、暗号化メッセージＥｂ１（Ｅｍ１（ｃ））＝（（ｃ）^{2} ）^{a1} ｍｏｄ　Ｎを作る。プロセスは次にステップ３０８に移行し、ここでＥｍ２（Ｅｍ１（ｃ））はトランシーバー・ユニット１３６を通してＭ１からＢ１に送られる。次に、ステップ３１０において、トランシーバー・ユニット１０４を通してＢ１からＥｍ２（Ｅｍ１（ｃ））を受け取った後、前述したようにＭ１の論理ユニット１１２はＤｍ１及びラビンのアルゴリズムを用いてＥｂ２（Ｅｍ１（ｃ））を解読する。Ｅｂ２（Ｅｍ１（ｃ））$^{1/2}$ ＝（（（ｃ）^{2} ）^{a2}）$^{1/2}$ 。作られたメッセージＤｍ１（Ｅｂ２（Ｅｍ１（ｃ））は（ｃ）^{a2}　ｍｏｄ　Ｎ、即ち暗号化メッセージＥｂ２（ｃ）に等しい。

【００４２】次に、ステップ３１２において、Ｍ１はトランシーバー・ユニット１０４を通して暗号化メッセージＥｂ１（ｃ）をＢ１に送り、ステップ３１４においてＢ１の処理装置１４０はＤｂ１を用いてＥｂ１（ｃ）を解読してＤｂ１（Ｅｂ１（ｃ））＝（（ｃ）^{a1}）^{b1}ｍｏｄ　Ｎ＝ｃを作る。処理装置１４０で通信メッセージｃが解読された後、プロセスはステップ３１６に移行し、ここで通信メッセージｃは基地局Ｂ１の制御ユニット１３８から陸線通信網１４２を通して基地局Ｂ２の制御ユニット１３０に送られる。Ｂ２とＭ２との間での通信メッセージｃの伝送は、Ｍ１及びＢ１の間での転送について述べたのと全く同様に行われ得る。それはステップ３１８－３３０で説明されており、それらはステップ３０２－３１４と同一であり、Ｂ２、Ｅｂ２、Ｄｂ２及びＡｂ２がＭ１、Ｅｍ１、Ｄｍ１及びＡｍ１に代わり、Ｍ２、Ｅｍ２、Ｄｍ２及びＡｍ２がＢ１、Ｅｂ１、Ｄｂ１及びＡｂ１に代わる。

【００４３】本発明の教示内容は前記の通信規格での使用のみに限定されると解されてはならず、類似の如何なるシステムをも包含すると解されるべきである。更に、上で明示的に開示した暗号化アルゴリズム以外の暗号化アルゴリズムを使用して本発明を実施してもよい。

【００４４】本発明は、その好ましい実施例に関して具体的に図示され解説されており、本発明の範囲から逸脱することなく形及び細部に変更を加え得ることが当業者に理解されるであろう。

【図面の簡単な説明】

【図１】本発明の実施例に従って構成された通信システムのブロック図である。

【図２】本発明の実施例の通信システム内でポイント間暗号化通信メッセージを提供するために行われるプロセスステップを示す流れ図である。

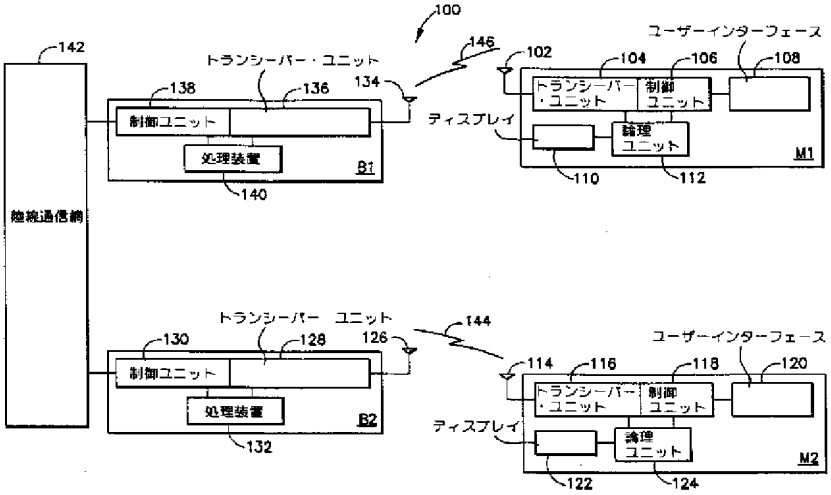
【図３】本発明の実施例の通信システム内で非ポイント間暗号化通信メッセージを提供するために行われるプロセスステップを示す流れ図である。

【符号の説明】

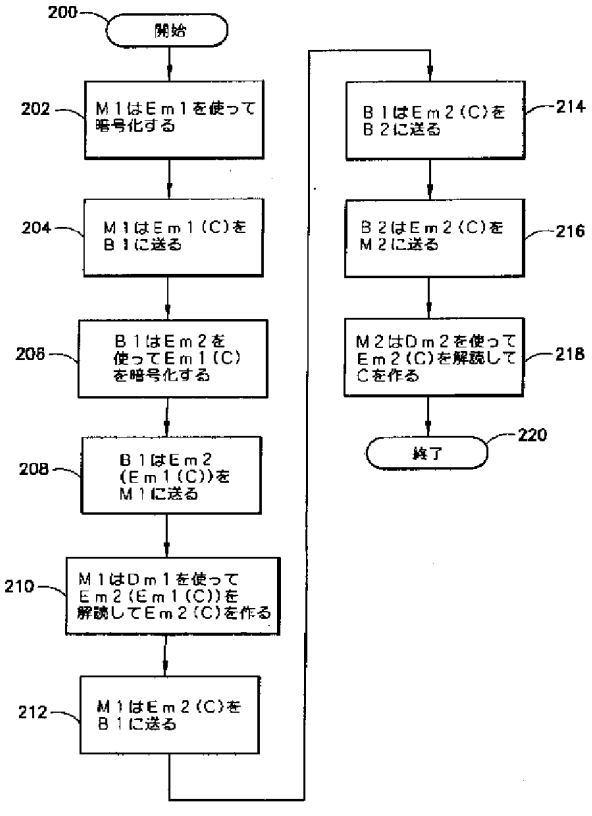
Ｂ１、Ｂ２…基地局

Ｍ１、Ｍ２…移動局

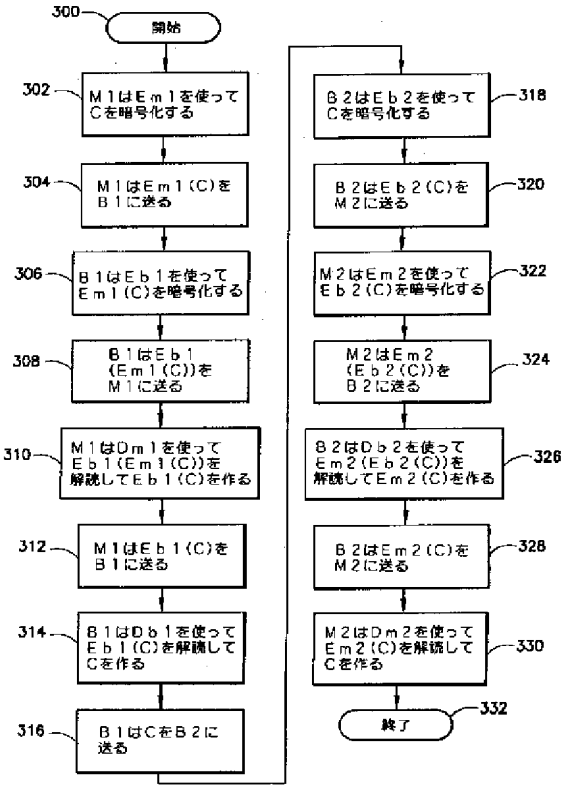
【図１】


100
142
145
102
ユーザーインターフェース
トランシーバー・ユニット
104
106
108
138
136
134
トランシーバー・ユニット
制御ユニット
制御ユニット
ディスプレイ
論理ユニット
処理装置
B1
M1
110
112
140
無線通信網
トランシーバー ユニット
144
130
128
126
ユーザーインターフェース
114
116
118
120
制御ユニット
トランシーバー・ユニット
制御ユニット
処理装置
B2
ディスプレイ
論理ユニット
M2
132
122
124

【図２】


200
開始
202
M1はEm1を使って暗号化する
204
M1はEm1(C)をB1に送る
206
B1はEm2を使ってEm1(C)を暗号化する
208
B1はEm2(Em1(C))をM1に送る
210
M1はDm1を使ってEm2(Em1(C))を解読してEm2(C)を作る
212
M1はEm2(C)をB1に送る
214
B1はEm2(C)をB2に送る
216
B2はEm2(C)をM2に送る
218
M2はDm2を使ってEm2(C)を解読してCを作る
220
終了

【図３】


300
開始
302
M1はEm1を使ってCを暗号化する
304
M1はEm1(C)をB1に送る
306
B1はEb1を使ってEm1(C)を暗号化する
308
B1はEb1(Em1(C))をM1に送る
310
M1はDm1を使ってEb1(Em1(C))を解読してEb1(C)を作る
312
M1はEb1(C)をB1に送る
314
B1はDb1を使ってEb1(C)を解読してCを作る
316
B1はCをB2に送る
318
B2はEb2を使ってCを暗号化する
320
B2はEb2(C)をM2に送る
322
M2はEm2を使ってEb2(C)を暗号化する
324
M2はEm2(Eb2(C))をB2に送る
326
B2はDb2を使ってEm2(Eb2(C))を解読してEm2(C)を作る
328
B2はEm2(C)をM2に送る
330
M2はDm2を使ってEm2(C)を解読してCを作る
332
終了